IN THE CLAIMS:

The text of all pending claims (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

Please AMEND claims 1, 8, and 15 and CANCEL claims 4, 11, 16 and 17, and ADD claims 18 and 19 in accordance with the following:

1. (CURRENTLY AMENDED) A cipher designing apparatus for designing cipher logic of a cipher device that effects cipher or decryption per block by using an F-function for converting input bits to output bits using a plurality of S-boxes, said cipher designing apparatus comprising:

an inputting unit inputting

a memory capacity of a high-speed referable memory provided to said cipher device,

an entire inputting and outputting bit number being input to and output from said cipher device, and

a minimum input and output bit number of said S-boxes as an initial value;

a tentative decision unit

dividing the entire input and output bit number by the initial value to acquire an integer quotient and an integer remainder,

making a first set composed of the integer quotient pieces of the initial value,

subtracting a number of one from the remainder integer number, when the remainder integer number is not zero, and adding the subtracted number of one to the initial value in the first set one by one until the integer remainder becomes zero, so as to acquire a second set composed of integer numbers, and

tentatively deciding the integer numbers in the second set as a tentative inputting and outputting bit number of S-box;

a combining unit

combining the integer numbers so as to make a third set of integer composed of combined integers;

a selecting unit ~~selecting an input and output bit number of said plurality of S-boxes~~

~~based on a memory capacity of a high-speed referable memory provided to said cipher device, a minimum input and output number of the S-boxes and an entire input and output number of the block, said selecting including determining an optimal combination of input and output bit numbers of each of the S-boxes for usable memory capacity of said memory; and~~

determining how many pieces of the combined integers are in the third set,

repeating the tentatively deciding, combining and determining until a number of the combined integer numbers becomes equal to a final number that is calculated based on the memory capacity and the entire inputting and outputting bit number, and

selecting, when the number of the combined integer numbers becomes equal to the final number, the combined integers of the third set to be an optimal combination of input and output bit numbers of each of the S-box

a S-box generating unit

generating a plurality of S-boxes each having the input and output bit number selected by said selecting unit.

2. (ORIGINAL) The cipher designing apparatus according to claim 1, further comprising a F-function generating unit which generates an F-function having said plurality of S-boxes generated by said S-box generating unit.

3. (ORIGINAL) The cipher designing apparatus according to claim 1, wherein said selecting unit selects the input and output bit number of each S-box in such a manner that a sum of sizes of said plurality of S-boxes becomes largest within a memory capacity of a primary cache memory installed in a processor provided to said cipher device.

4. (CANCELLED)

5. (ORIGINAL) The cipher designing apparatus according to claim 1, further comprising a smallest input and output number specifying unit which specifies a smallest value of the input and output number of said plurality of S-boxes.

6. (CURRENTLY AMENDED) The cipher designing apparatus according to claim [[4]]1, wherein ~~said combining unit completes combining of the input and output numbers based on a final value determined by the entire input and output bit number of said block and the~~

~~memory capacity of said~~ the high-speed referable memory is a primary cache memory.

7. (CURRENTLY AMENDED) The cipher designing apparatus according to claim [[4]]1, wherein said tentative decision unit tentatively decides the input and output number of each S-box by allocating said remainder, if there is any, to the input and output numbers of the S-boxes that are placed apart at remotest positions.

8. (CURRENTLY AMENDED) A cipher designing method for designing cipher logic of a cipher device that effects cipher or decryption per block by using an F-function for converting input bits to output bits using a plurality of S-boxes, the method comprising:

inputting

a memory capacity of a high-speed referable memory provided to said cipher device,

an entire inputting and outputting bit number being input to and output from said cipher device, and

a minimum input and output bit number of said S-boxes as an initial value;

dividing the entire input and output bit number by the initial value to acquire an integer quotient and an integer remainder;

making a first set composed of the integer quotient pieces of the initial value;

subtracting a number of one from the remainder integer number, when the remainder integer number is not zero, and adding the subtracted number of one to the initial value in the first set one by one until the integer remainder becomes zero, so as to acquire a second set composed of integer numbers;

tentatively deciding the integer numbers in the second set as a tentative inputting and outputting bit number of S-box;

combining the integer numbers so as to make a third set of integer composed of combined integers;

determining how many pieces of the combined integers are in the third set;

repeating the tentatively deciding, combining and determining until a number of the combined integer numbers becomes equal to a final number that is calculated based on the memory capacity and the entire inputting and outputting bit number;

~~selecting an input and output bit number of said plurality of S-boxes based on a memory capacity of a high-speed referable memory provided to said cipher device, a minimum input and~~

~~output number of the S-boxes and an entire input and output number of the block, said selecting including determining an optimal combination of input and output bit numbers of each of the S-boxes for usable memory capacity of said memory~~selecting, when the number of the combined integer numbers becomes equal to the final number, the combined integers of the third set to be an optimal combination of input and output bit numbers of each of the S-box; and

generating a plurality of S-boxes each having the input and output bit number selected.

9. (PREVIOUSLY PRESENTED) The cipher designing method according to claim 8, further comprising:

generating an F-function having said plurality of S-boxes generated.

10. (PREVIOUSLY PRESENTED) The cipher designing method according to claim 8, wherein when the input and output bit number are selected, the input and output bit number of each S-box is selected in such a manner that a sum of sizes of said plurality of S-boxes becomes largest within a memory capacity of a primary cache memory installed in a processor provided to said cipher device.

11. (CANCELLED)

12. (PREVIOUSLY PRESENTED) The cipher designing method according to claim 8, further comprising :

specifying a smallest value of the input and output number of said plurality of S-boxes.

13. (CURRENTLY AMENDED) The cipher designing method according to claim ~~11~~8, wherein ~~the combining is completed based on a final value determined by the entire input and output bit number of said block and the memory capacity of said~~ the high-speed referable memory is a primary cache memory.

14. (CURRENTLY AMENDED) The cipher designing method according to claim ~~11~~8, wherein when tentatively deciding input and output number, the input and output number of each S-box is tentatively decided by allocating said remainder, if there is any, to the input and output numbers of the S-boxes that are placed apart at remotest positions.

15. (CURRENTLY AMENDED) A computer readable medium for storing instructions, which when executed by a computer, causes the computer to realizes a cipher designing method for designing cipher logic of a cipher device that effects cipher or decryption per block by using an F-function for converting input bits to output bits using a plurality of S-boxes, the method comprising:

inputting

a memory capacity of a high-speed referable memory provided to said cipher device,

an entire inputting and outputting bit number being input to and output from said cipher device, and

a minimum input and output bit number of said S-boxes as an initial value;

dividing the entire input and output bit number by the initial value to acquire an integer quotient and an integer remainder;

making a first set composed of the integer quotient pieces of the initial value;

subtracting a number of one from the remainder integer number, when the remainder integer number is not zero, and adding the subtracted number of one to the initial value in the first set one by one until the integer remainder becomes zero, so as to acquire a second set composed of integer numbers;

tentatively deciding the integer numbers in the second set as a tentative inputting and outputting bit number of S-box;

combining the integer numbers so as to make a third set of integer composed of combined integers;

determining how many pieces of the combined integers are in the third set;

repeating the tentatively deciding, combining and determining until a number of the combined integer numbers becomes equal to a final number that is calculated based on the memory capacity and the entire inputting and outputting bit number;

~~selecting an input and output bit number of said plurality of S-boxes based on a memory capacity of a high-speed referable memory provided to said cipher device, a minimum input and output number of the S-boxes and an entire input and output number of the block, said selecting including determining an optimal combination of input and output bit numbers of each of the S-boxes for usable memory capacity of said memory~~selecting, when the number of the combined integer numbers becomes equal to the final number, the combined integers of the third set to be an optimal combination of input and output bit numbers of each of the S-box; and

generating a plurality of S-boxes each having the input and output bit number selected.

16. (CANCELLED)

17. (CANCELLED)

18. (NEW) The cipher designing apparatus according to claim 1, wherein said final number is calculated by an integer portion of ((the entire input and output bit number)/$\log_2$ (a size of the high-speed referable memory)) +1.

19. (NEW) The cipher designing method according to claim 8, wherein said final number is calculated by an integer portion of ((the entire input and output bit number)/$\log_2$ (a size of the high-speed referable memory)) +1.